SERVICENOW PROJECT SUBMISSON

ACCESS CONTROL FOR PROJECT TABLE

Submitted by

Kethu Charan Kumar Reddy au723921244024

Kataru Sreenath Reddy au723921244023

Poli Tejeswar Reddy au723921244040

Dandugula Naveen au723921244014

Arjun College of Technology , Coimbatore

Anna University Chennai -600 025

ACCESS CONTROL FOR PROJECT TABLE

Project Overview :

The goal of this project is to implement a robust access control system for a project table that stores sensitive information related to various projects. The system will ensure that only authorized users can access, modify, or delete project data based on their roles and permissions. This will enhance data security, streamline collaboration, and ensure compliance with organizational policies

Objective:

Assign different levels of access to the project table based on user roles to ensure that users only perform actions that are appropriate for their role.

- **Example Roles**:
    - **Admin**: Full access to create, read, update, delete, and manage user permissions.
    - **Project Manager**: Ability to create, update, delete, and assign projects, but no access to manage other users or roles.
    - **Team Member**: Limited to reading and commenting on project data.
    - **Guest**: View-only access to specific, public project data.

1. **Implement Granular Permissions**

- **Objective**: Fine-tune access to specific operations (e.g., create, read, update, delete) at the project table level based on user role.
- **Example**:
    - Ensure that users with the "Team Member" role can view project details but cannot update or delete project information.
    - Restrict the "Admin" role to only edit user roles and permissions, not project data unless necessary.

2. **Minimize the Risk of Unauthorized Access**

- **Objective**: Protect the project table from unauthorized access by enforcing strict authentication and authorization checks.
- **Example**:
    - Users should not be able to bypass authentication.
    - Implement strong password policies, multi-factor authentication (MFA), or other security mechanisms to prevent unauthorized users from accessing the system.

3. **Ensure Data Integrity and Protection**

- **Objective**: Ensure that users can only modify or delete project data when they are authorized to do so and that their actions are logged for accountability.
- **Example**:

- Project Managers should only be able to edit projects they are associated with or authorized to manage.
- Use validation checks to prevent unauthorized data manipulation.
- Log all access attempts, including changes to project data, for auditing purposes.

Access Levels:

1. Project Manager (PM): Full access (create, read, update, delete)
2. Team Members: Read and update access (task assignments, status updates)
3. Stakeholders: Read-only access (project overview, progress)
4. External Partners: Limited read-only access (specific project details)

Access Control Rules:

1. PM can create, update, and delete projects.
2. Team members can update task assignments and status.
3. Stakeholders can view project overview and progress.
4. External partners can view limited project details.

Key Feactures and concept used:

1. Regularly review access permissions

2. Use strong passwords and encryption

3. Limit access to sensitive data

4. Monitor audit logs

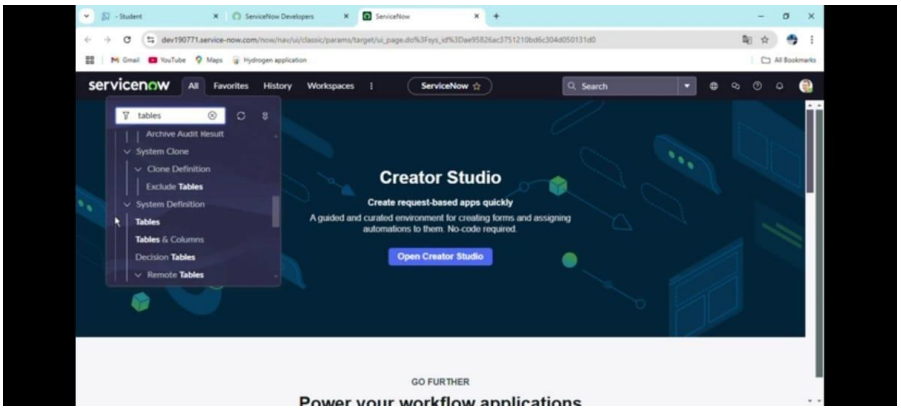
Detailed Steps To Solution Design :

Implementation :

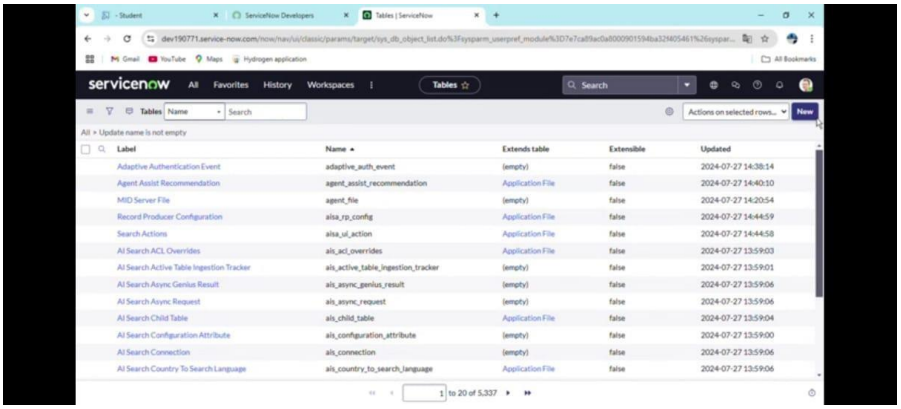
Step 1: Sign up for a developer account on the ServiceNow Developer site

Step 2: Open Instance

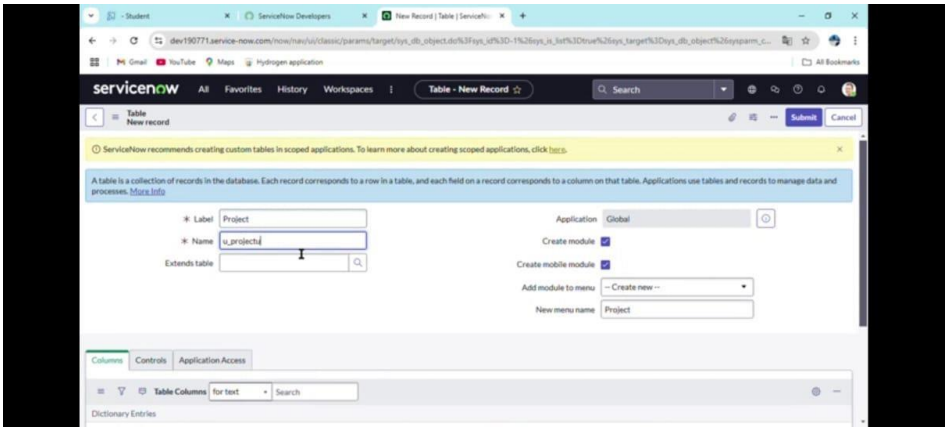
Step 3: In All>>Tables



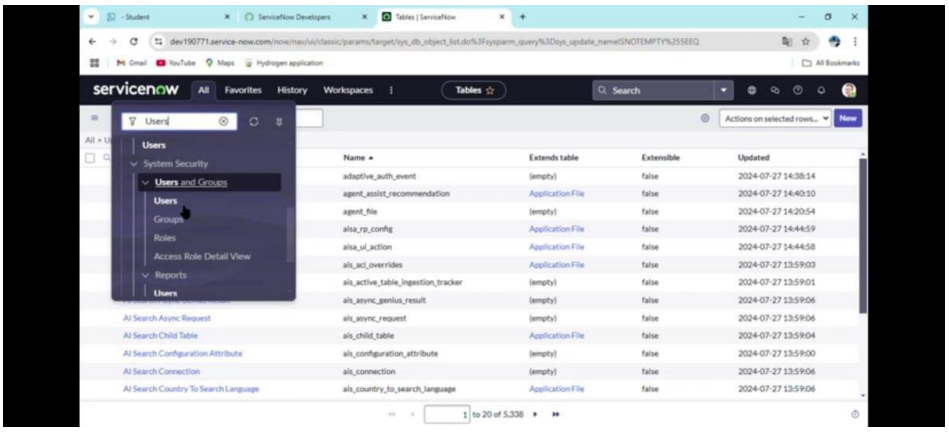
Step 4: Click>>New



Step 5: Fill The Details And Click Submit

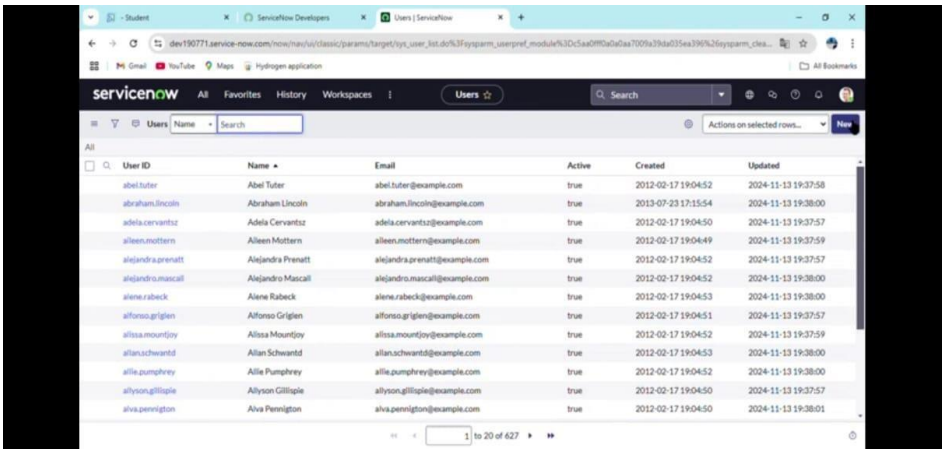


Step 6: In All>>Users

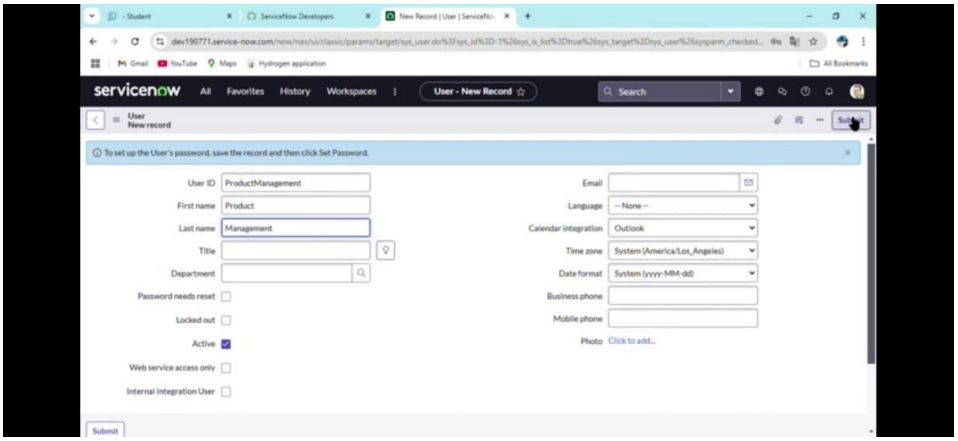


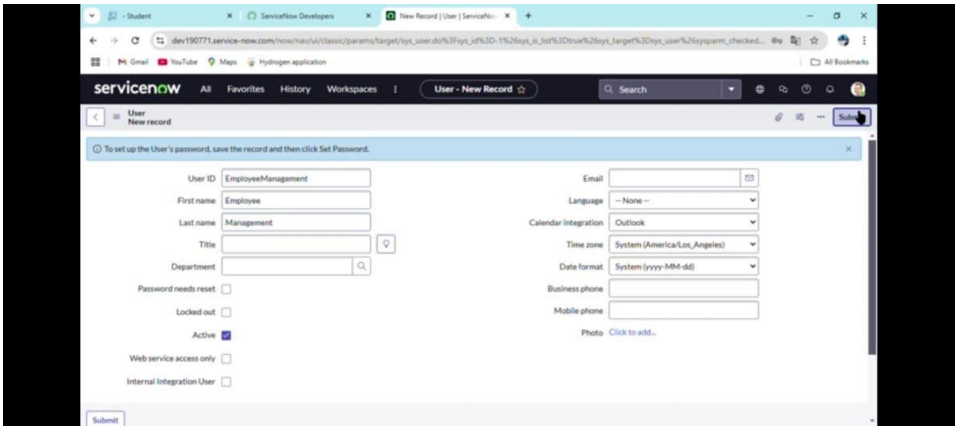
Step 7: Click>>New

Create Two Users Product Manager and Employe Management

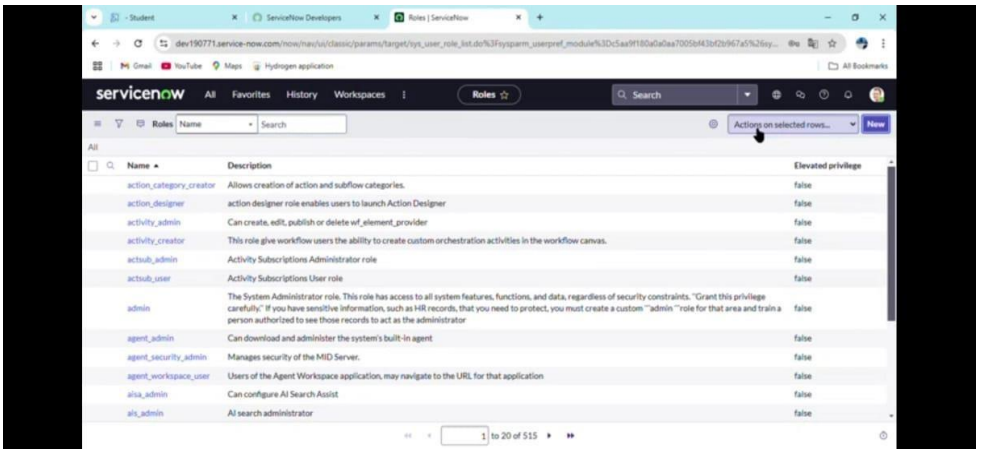


Step 8: Fill The Details And Click>>Submit

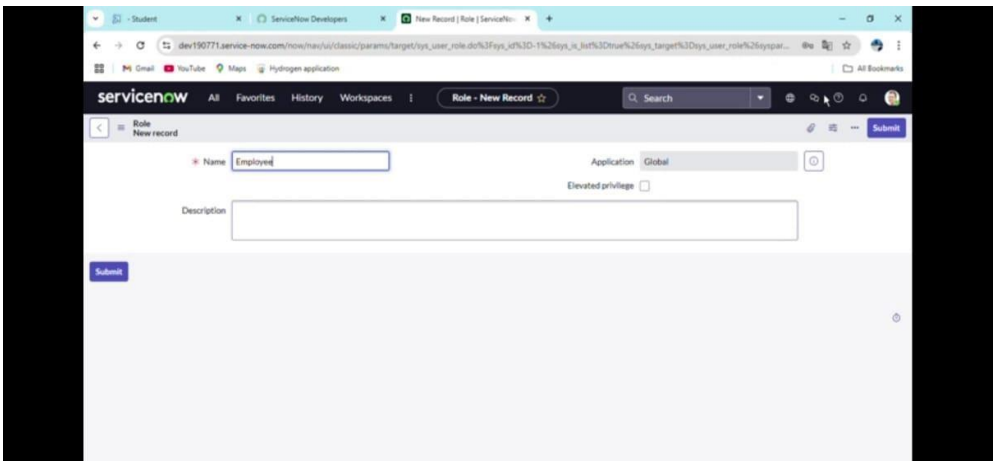




Step 9: Open Role >>New

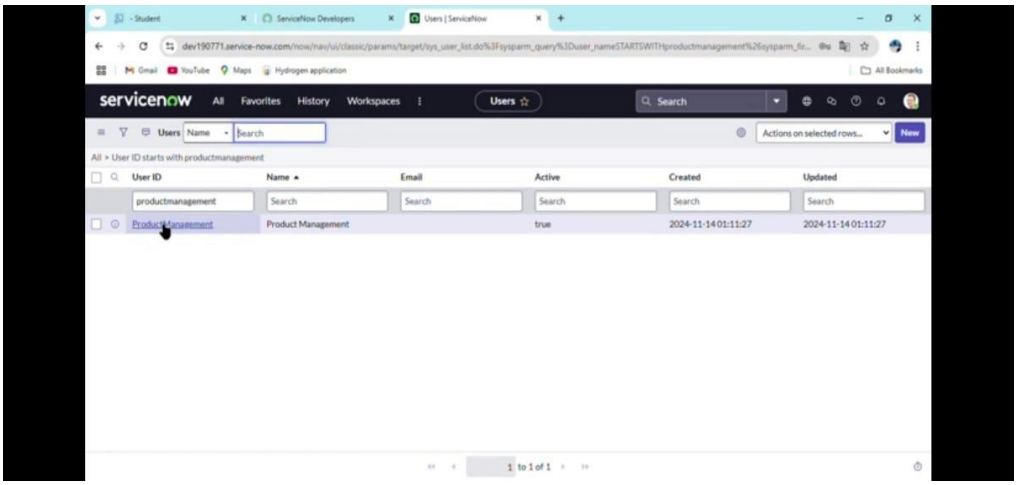


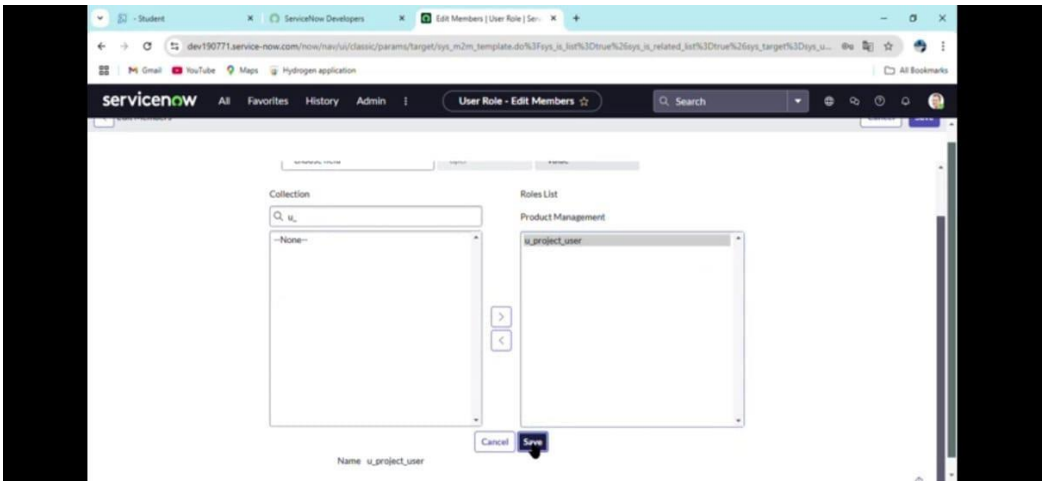
Step 10: Create Employee Role



Step 11: In All>>Users>>Search Product Management

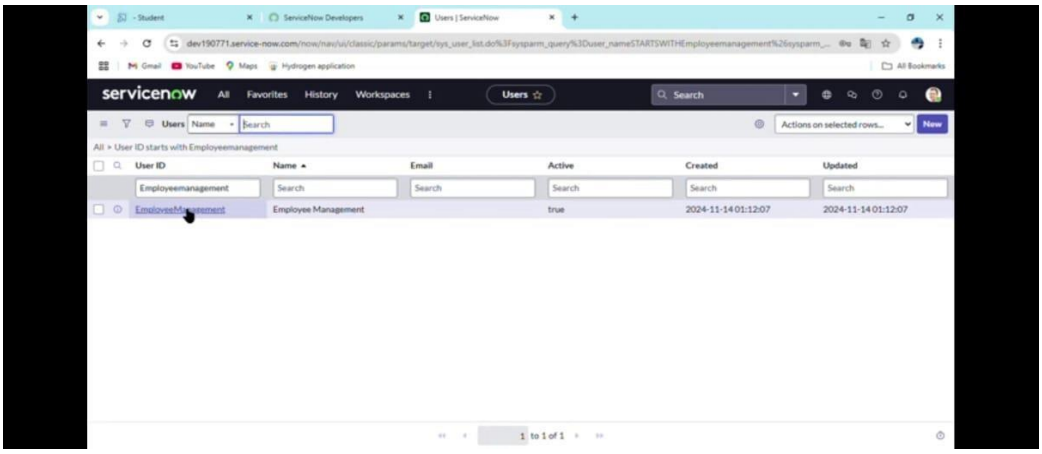
And add Role to it



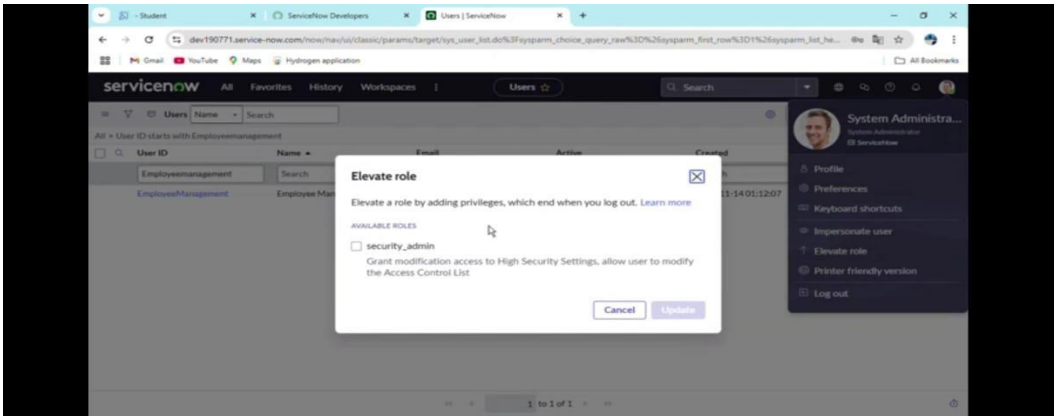


Step 12: In All>>Users>>Search EmployeeManagement

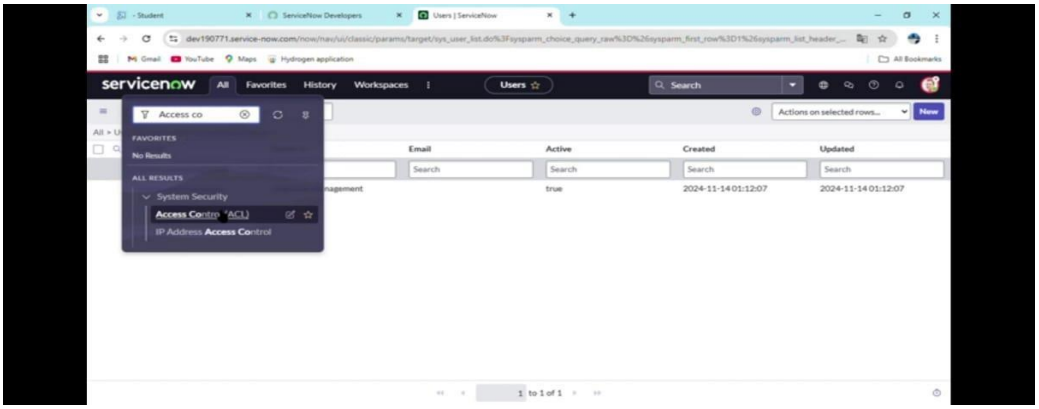
And add Role to it

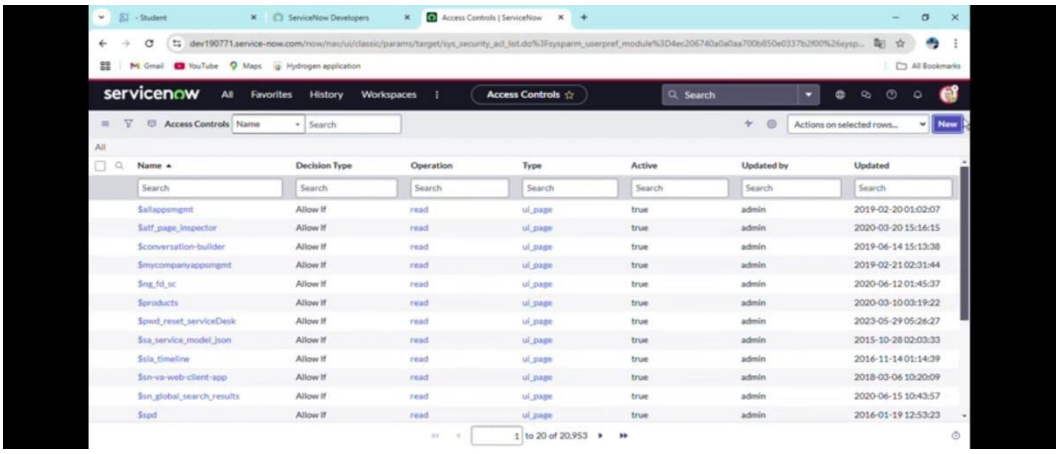


Step 13: Click on the Profile avatar >> Elevate Role >> Grant the high security

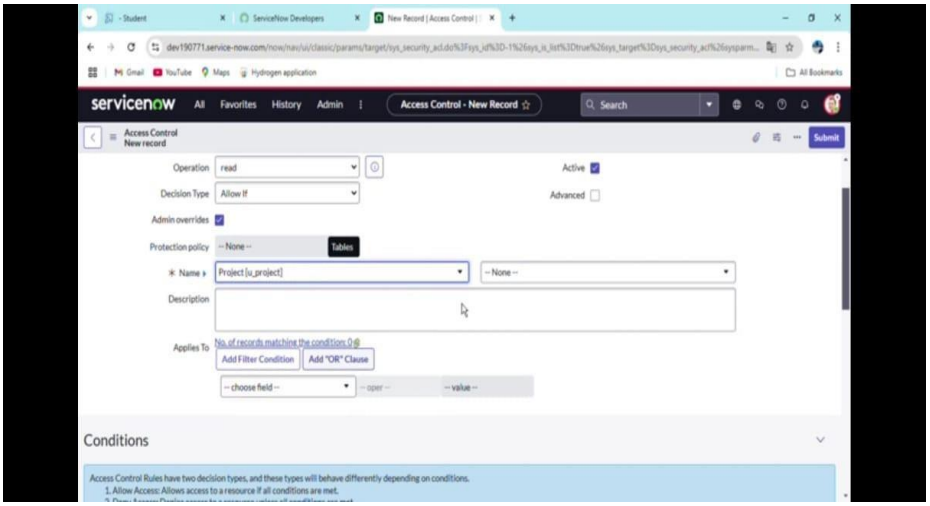


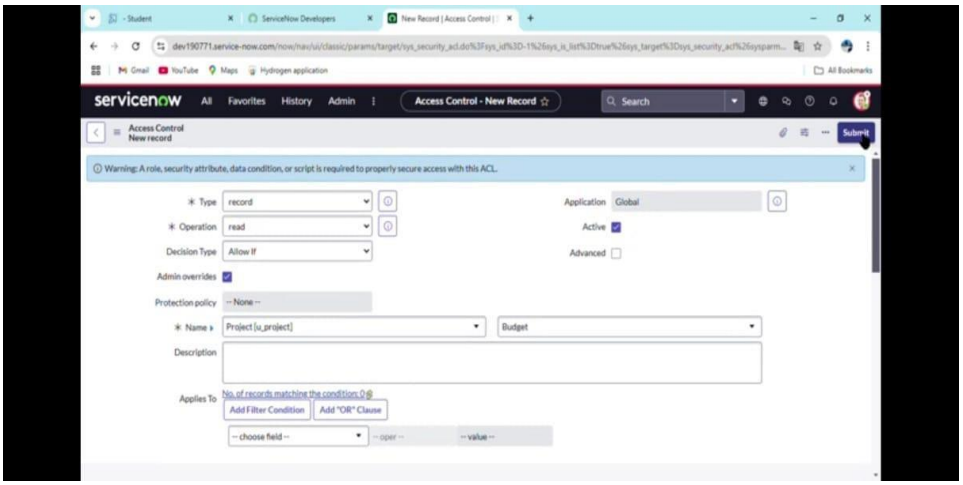
Step 14: In All>> Search & Open ACL >> New

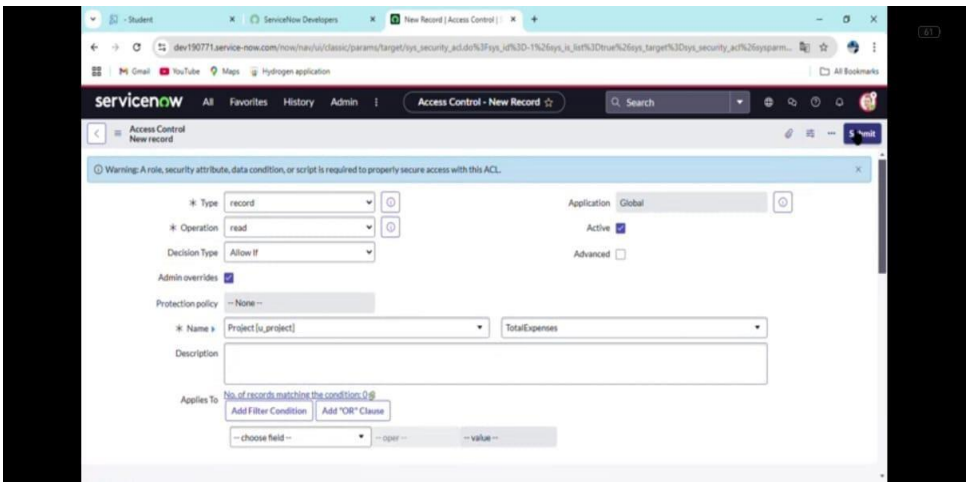




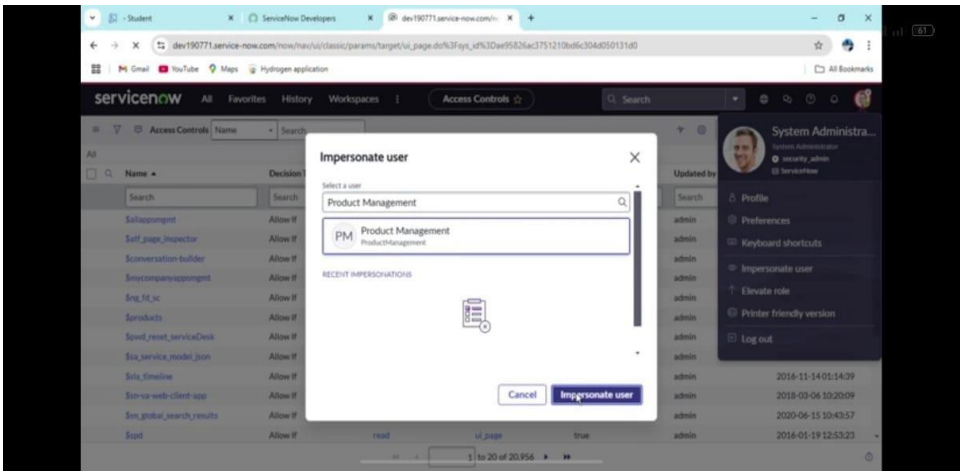
Step 15: Fill the details below and Create Read Operation Table Level ACL(none) on Employee role >> Save



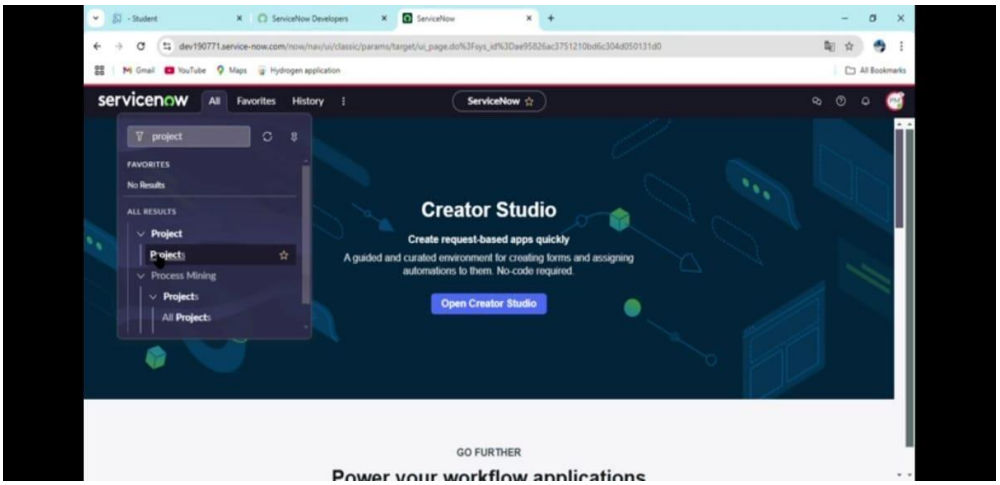




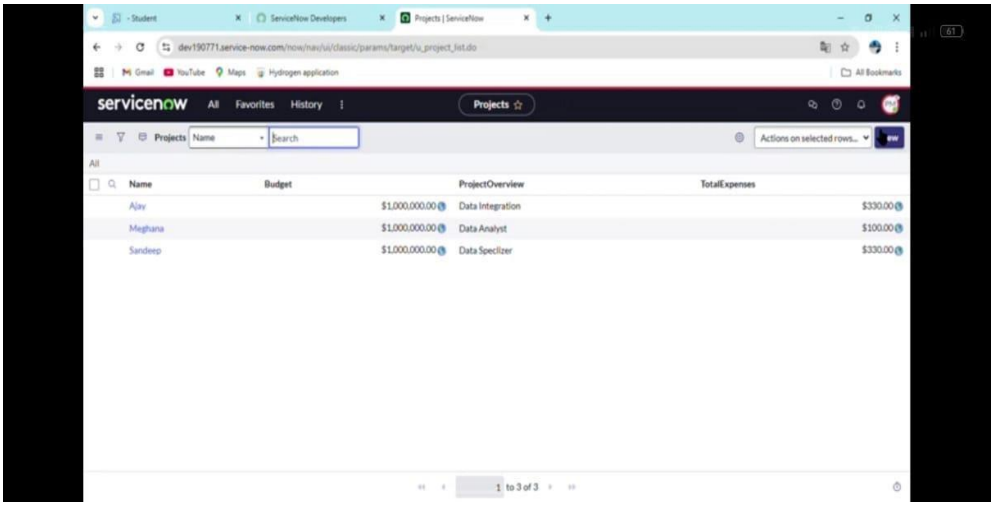
Step 16: Impersonate User >> Product Management



Step 17: All>>Project>>New



Step 18: Create 3 Records with any details



Testing and Validation:

Test User Authentication

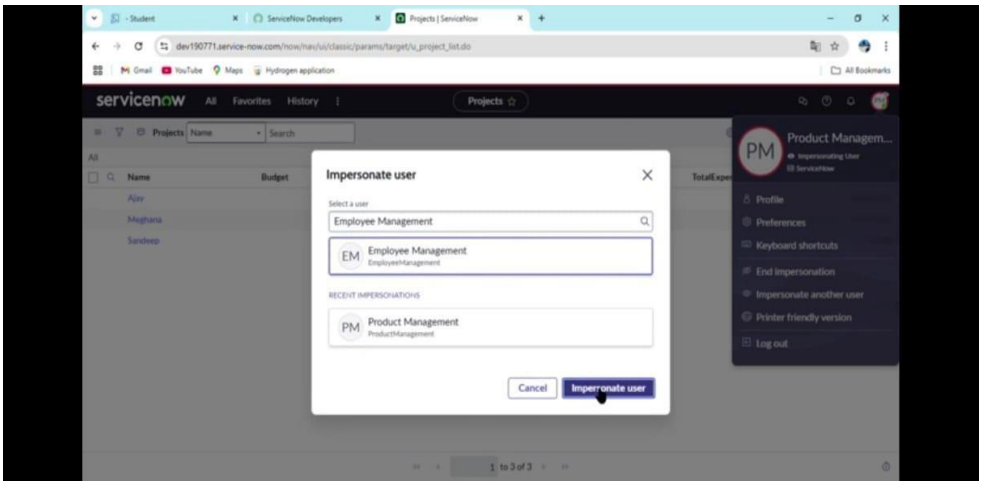
- Ensure that users can only access the project table after successful authentication (e.g., login with username and password).
- Test invalid login attempts and ensure that users cannot access the table without proper credentials.
- Verify session expiration behavior (if applicable).

Validation:

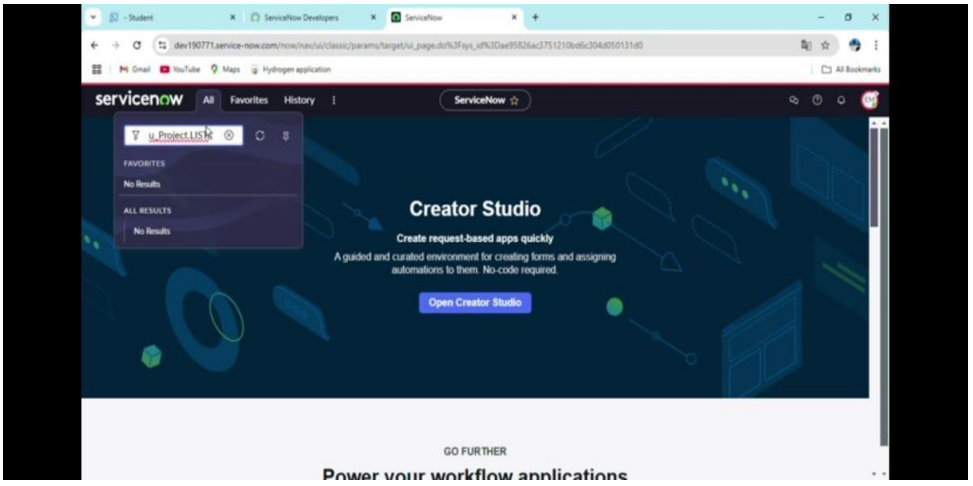
When testing and validating access control for a project table, the goal is to ensure that only authorized users can access, modify, or manage the project table data according to defined roles and permissions. Proper access control testing helps protect sensitive data and ensures that users' actions are consistent with their designated permissions**.**

Result:

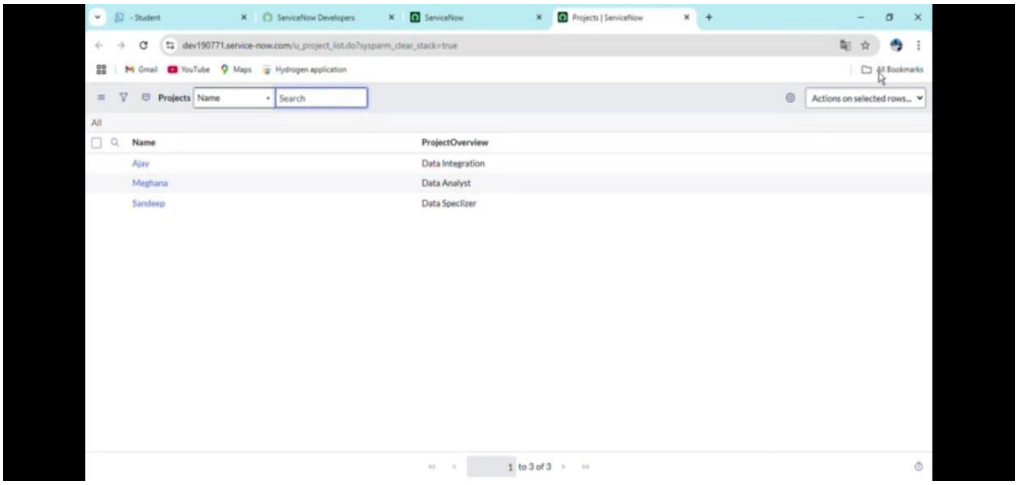
Step 1: Impersonate User >> Employee Management



Step 2: All >> u_project.LIST

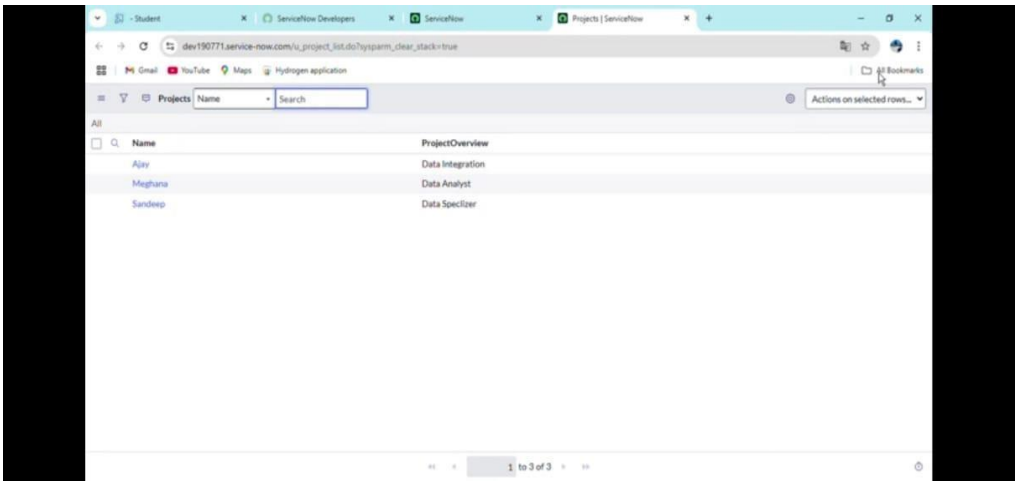


Step 3:



In the figure above, we can ensure that some fields(Budget,Total Expenses) visibility is restricted for employees on the Project table

OUTPUT:



Conclusion: Implementing access control for a project table ensures the security, integrity, and confidentiality of project data. By assigning roles and permissions, project managers Thus The Project “Access control for project Table” has been implemented successfully